What Can Security-Critical Engineering *learn from* Safety-Critical Engineering?

NDIA Symposium

June, 2003

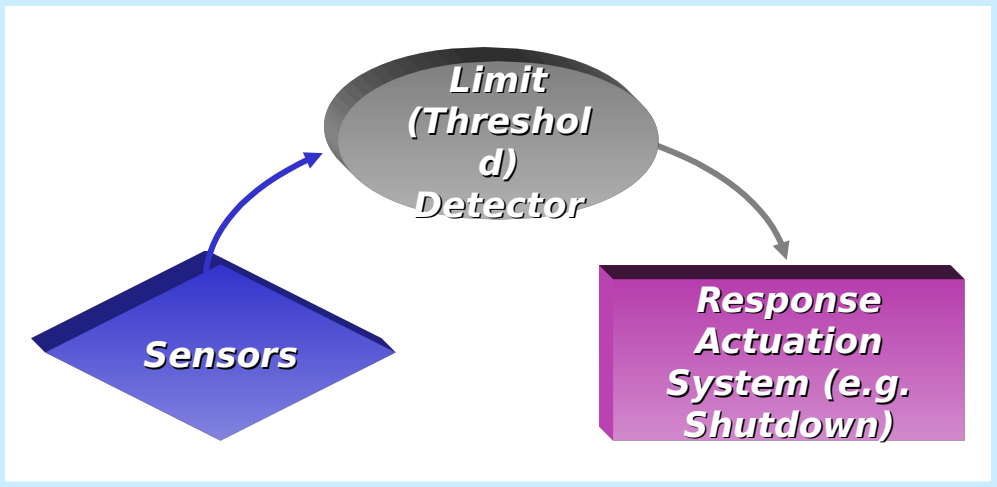
Gerald R. Larocque, Ph.D.
TIAX LLC
larocque.g@tiax.biz

Sean Martin, Ph.D.
Genspire, Ltd.
Sean.martin@genspire.com

Copyright © 2003 TIAX LLC,

Historical experience in safety critical systems has led to a careful, systematic approach to design and analysis.

- Safety critical components
  - temperature sensors
  - threshold detector
  - actuators
  - robust fault tolerant design

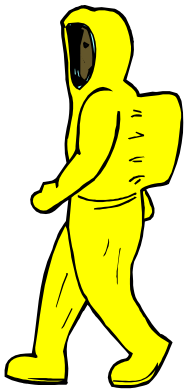


How would you expect this to be designed?

 © Tiax LLC & Genspire, LTD 2003

Good practice in safety engineering follows several principles that are applicable to critical systems in general.

- Careful segregation of system functions
- Systematic identification of potential failures
- Characterization and quantification of risks
- Design of risk/hazard mitigation measures
- Assessment of effectiveness of mitigation measures
- Analysis of safety system reliability



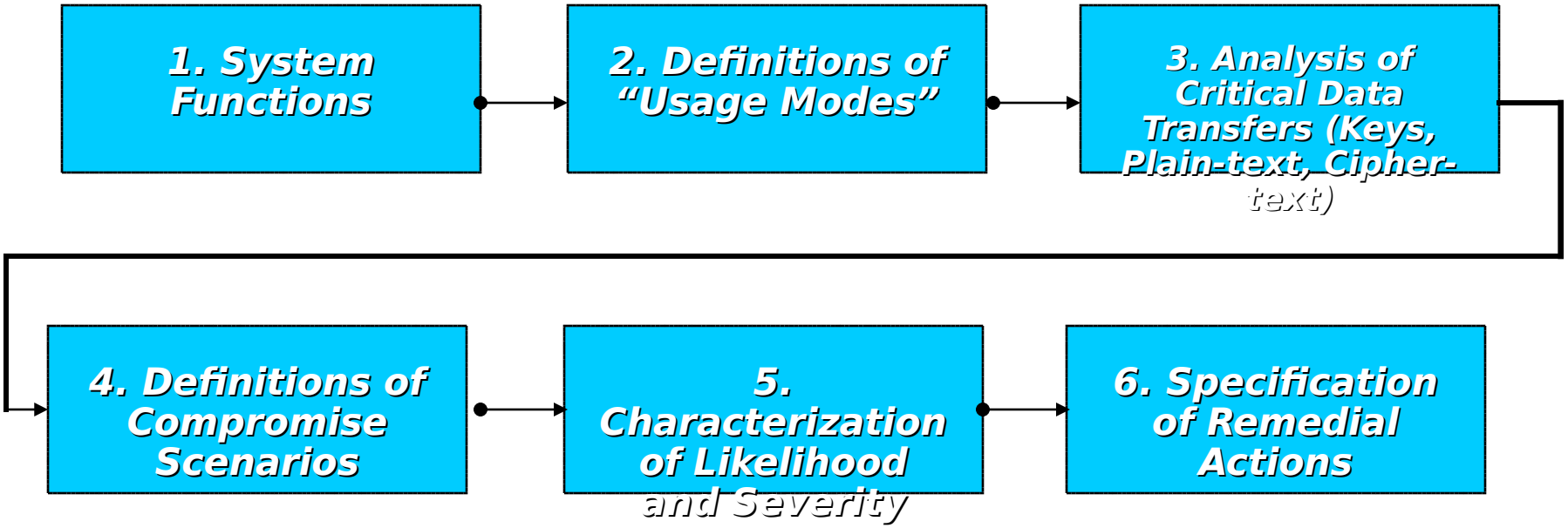
 © Tiax LLC & Genspire, LTD 2003

Several key security issues are highlighted by the "Cain" principles that comprise major functions of electronic security systems.

Confidentiality	*Can others observe our communications?*
Authentication	*How do I know that I am communicating with the person I think I am?*
Integrity	*Can someone tamper with my message?*
Non-repudiation	*Once agreed, can the communication be disputed?*

 © Tiax LLC & Genspire, LTD 2003

An overall system security review can go far to increase the difficulty of compromise and thus, to identify and close the "back door."

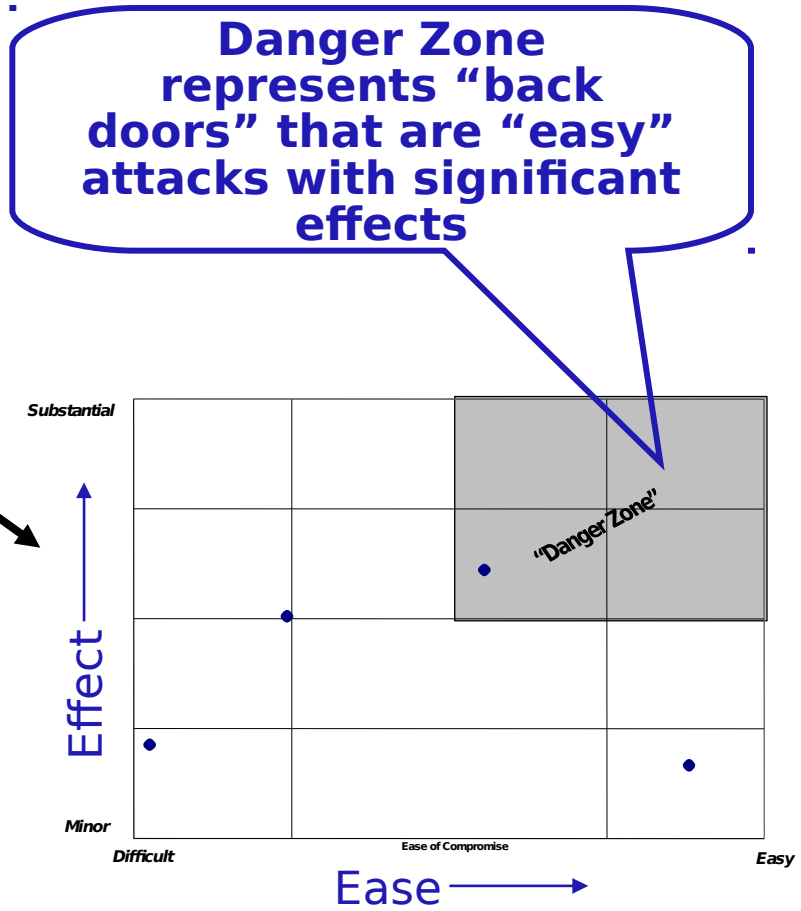

1. System Functions
2. Definitions of "Usage Modes"
3. Analysis of Critical Data Transfers (Keys, Plain-text, Cipher-text)
4. Definitions of Compromise Scenarios
5. Characterization of Likelihood and Severity
6. Specification of Remedial Actions

 © Tiax LLC & Genspire, LTD 2003

A formal analysis to identify threats in a standard form has proven a useful analysis tool and leads to an instructive graphical presentation.

For example:

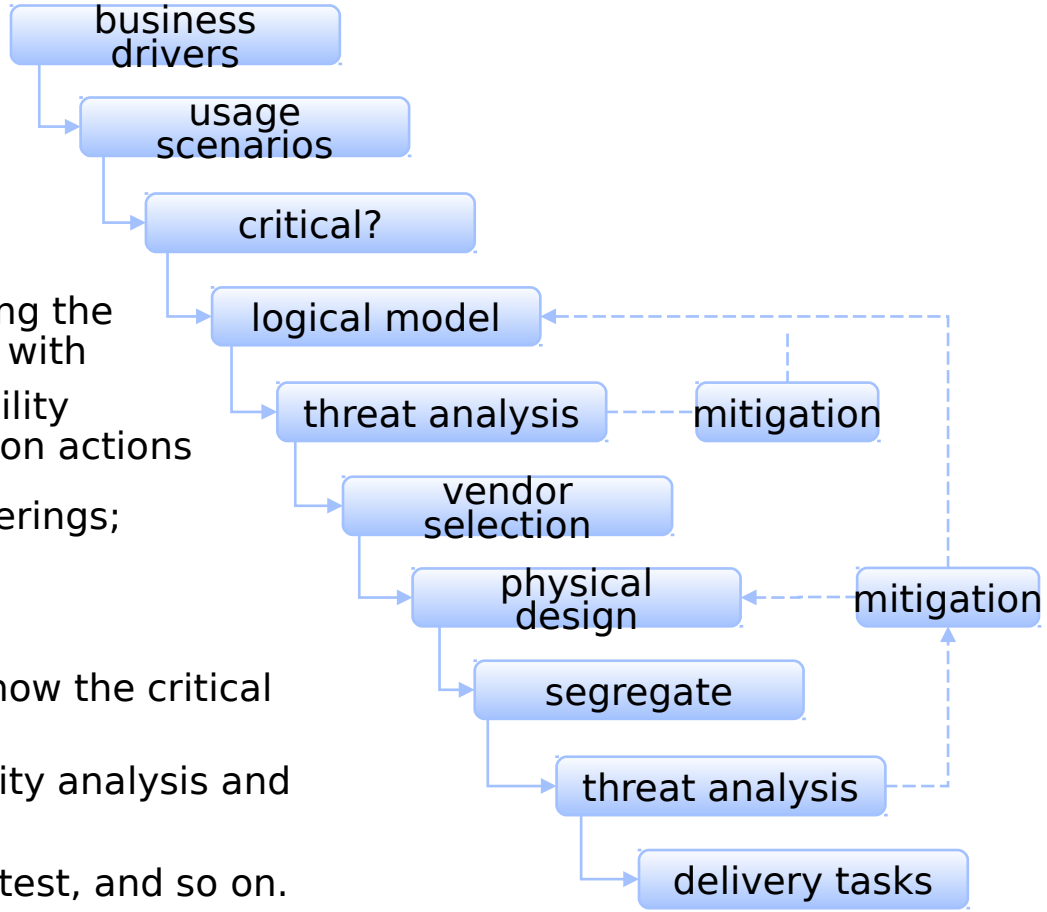
T n	*Reference Figure: i*	*Usage Scenario*	*Title*	
Impact		• Ease: X	• Propagation: Y	• Remediation: Z
Consequence		**Description of Consequence**		
Secrets Involved	Primary	• *Primary Secret to be compromised*		
	Scope	• *How widespread is the result of the compromise*		
	Secondary	• *Any secondary secrets that are compromised*		
Mechanism		• Description of method of compromise/attack • Description of required skills • Description of required technology		
Remediation		• What must system user/administrator do to recover?		
Comment		• General Observations, including method of propagation		



 © Tiax LLC & Genspire, LTD 2003

Several practical steps are generally required to secure business processes, many of which are analogous to safety system design and analysis.

- Establish the business drivers
- Analyse & define usage scenarios
- Identify the critical scenarios, for example, where disputes could arise;
- Produce a logical model meeting the usage scenarios and buildable with OTS products
- Conduct a threat and vulnerability analysis, and consider mitigation actions
- Assess and select vendors' offerings;
- Produce a physical design;
- Now segregate it focusing on how the critical usage scenarios are delivered;
- Repeat a threat and vulnerability analysis and mitigation actions; and
- Now go build it, and of course test, and so on.



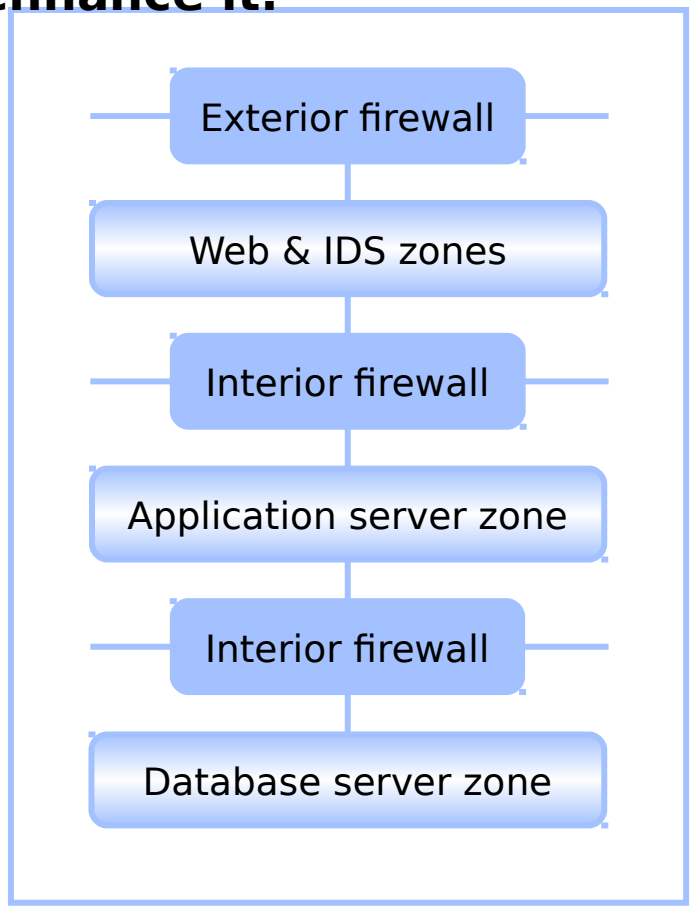
 © Tiax LLC & Genspire, LTD 2003

By partitioning the design into distinct security "zones," design activities may be appropriately focussed.

High Integrity zone	Production engineering zone
• The scope is kept as small as possible and limited to critical functionality	• The scope may naturally be extensive
• Rarely updated	• May undergo continual updates
• Stringent configuration management and control processes are applied, e.g., all s/w and h/w subject to peer review processes.	• Regular configuration management and control processes are applied
• The highly controlled functionality produces records that can be implicitly trusted.	• Produces tamper-evident records – designed so that any tamper will result in an observable discrepancy
• Highly restricted access thus denying opportunities for attacks by internal staff	• Regular zoning access controls
• Reporting without requiring administrator access or intervention, for example, performance, heart-beats, resource usage, log files, etc.	• Regular zoning access controls

 © Tiax LLC & Genspire, LTD 2003

Although a common IT network architecture provides effective security, “safety-critical” methods may help to enhance it.

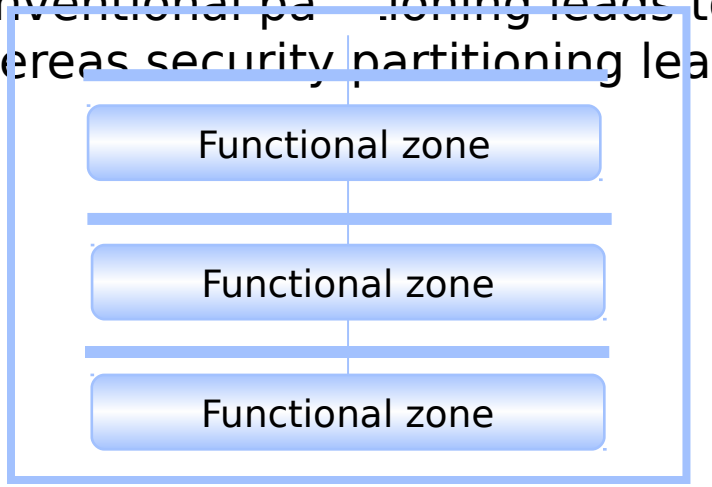


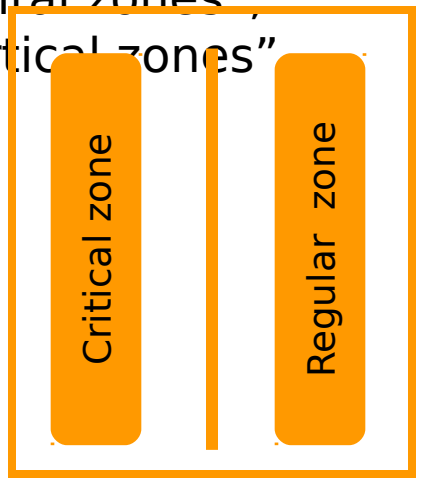
- A standard, layered architecture is often structured similar to that shown.
  - An exterior facing firewall with IDS
  - Three internal server layers with web servers, application servers and database servers
  - Two internal firewall layers between the three layers.
- By design, this layered approach requires an intruder to progressively surmount firewalls to reach increasingly critical areas.
- Although this is a good practice, it may be possible to enhance it.

 © Tiax LLC & Genspire, LTD 2003

Despite its attractive architecture, this partitioning suffers from several limitations from a security standpoint.

- The partitioning is based on functional rather than security considerations
  - By analogy, using this approach, a reactor system might group sensors in one zone; control logic in a 2nd zone and response actuators in a 3rd zone
  - These zones do not relate to critical usage functions and thus complicate securing the system
- Conventional partitioning leads to "horizontal zones", whereas security partitioning leads to "vertical zones"

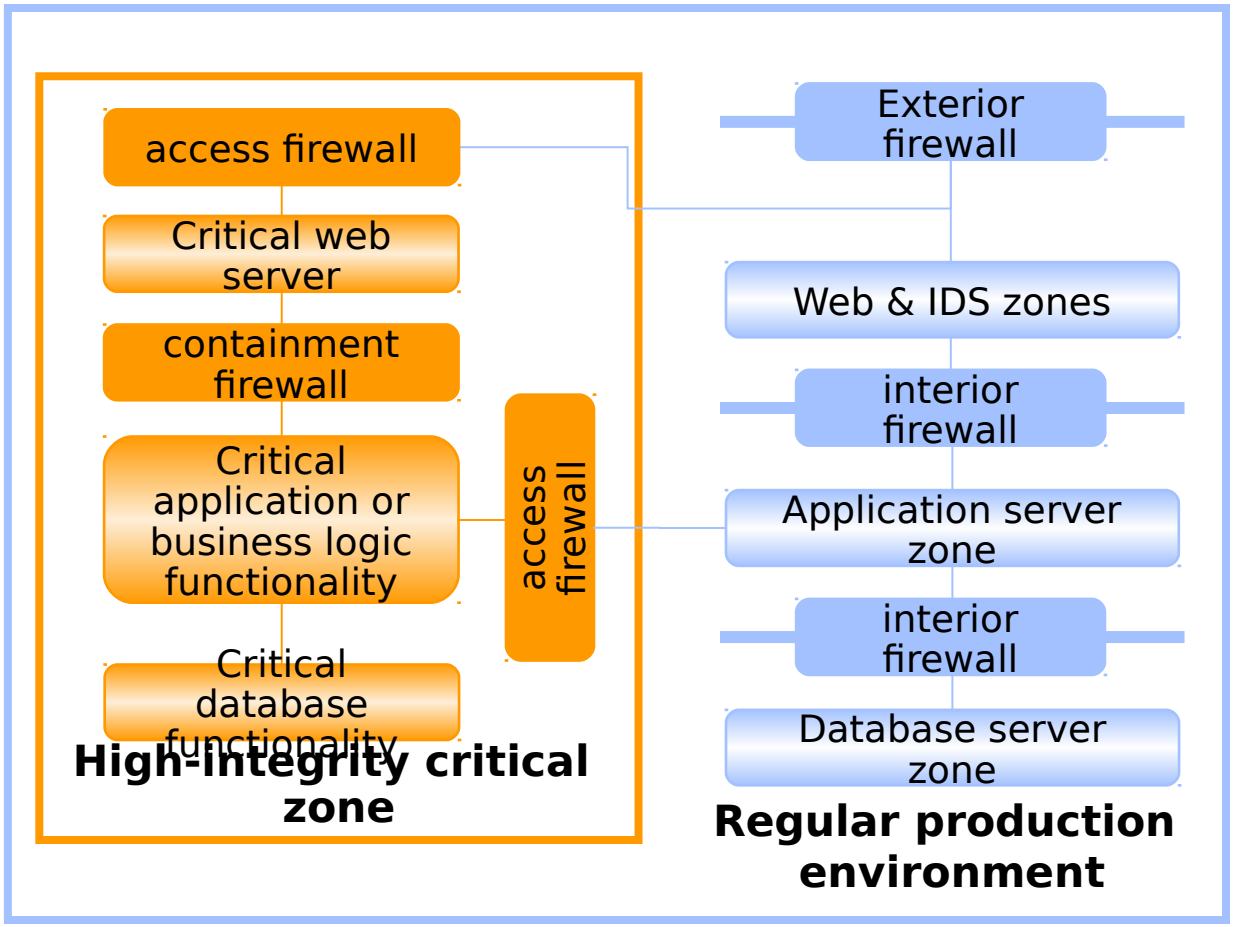




 © Tiax LLC & Genspire, LTD 2003

By applying safety-like considerations, a more defensible partitioning may be realized.

- Isolates "production" or working environment from "critical zone"
- Surrounds critical zones with resilient firewalls
- Locally contains compromise
- Electronic "fingerprints" detect compromise



 © Tiax LLC & Genspire, LTD 2003

Although conventional approaches provide effective security, it appears likely that the most critical systems can benefit from enhanced partitioning methods.

- By learning from safety engineering, a criticality based partitioning can be realized.
- Similar to safety engineering, formal analysis and characterization can be used to guide design.
- Effective mediation measures can be designed and enhanced through analysis of effectiveness.
- Resulting system should exhibit enhanced security
- Keeping the critical zone design simple is crucial: “KISS—Keep It Small and Simple”

The message is not new:

“He who defends everything, defends nothing”

—Frederick the Great

 © Tiax LLC & Genspire, LTD 2003